MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

SUPPLEMENTARY EXAMINATION

TRIMESTER 1, 2015/2016

TSN3251 – COMPUTER SECURITY

(All Sections / Groups)

18 NOV 2015
9.00 AM – 11.00 AM
(2 HOURS)

INSTRUCTIONS TO STUDENTS

1. This paper consists of 7 pages (including cover page) with 5 Questions only.
2. Attempt **ALL FIVE** questions. The distribution of the marks for each question is given. This paper carries **100 marks**.
3. Please print all your answers in the Answer Booklet provided.

Question 1 (20 Marks)

a) A computer security threat is blocked by the controls you put in place on your system's vulnerability. The controls that are put into place are the defence mechanisms and the simplest mechanism is to prevent access to the vulnerability. State and give a brief description of the other FOUR (4) defence mechanisms.

[8 marks]

b) In order for a person to conduct a malicious attack, what are the three (3) areas that he or she needs to have?

[3 marks]

c) If plaintext is denoted by P, ciphertext is denoted by C, the encryption function is denoted by E( ) and the encryption key is denoted by K_s, write down the formal notation relating plaintext and ciphertext.

[2 marks]

d) Define Encryption.

[1 mark]

e) Differentiate between Steganography and Cryptography.

[2 marks]

f) What is meant by the statement "In symmetric cryptography, both the sender and the receiver are equal whereas in asymmetric cryptography, both parties (sender and receiver) are not equal"?

[4 marks]

Continued ...

Question 2 (20 Marks)

a) State the Principle of Adequate Protection.

[1 mark]

b) Decrypt the following message that was encrypted using the Playfair cipher with the key "delicious". Ensure that you show each step you did to decrypt it clearly.

ASHQCYORKBLY

[6 marks]

c) Encrypt the following using a 3 row rail fence cipher. Ensure that you clearly show the steps you used to encrypt it.

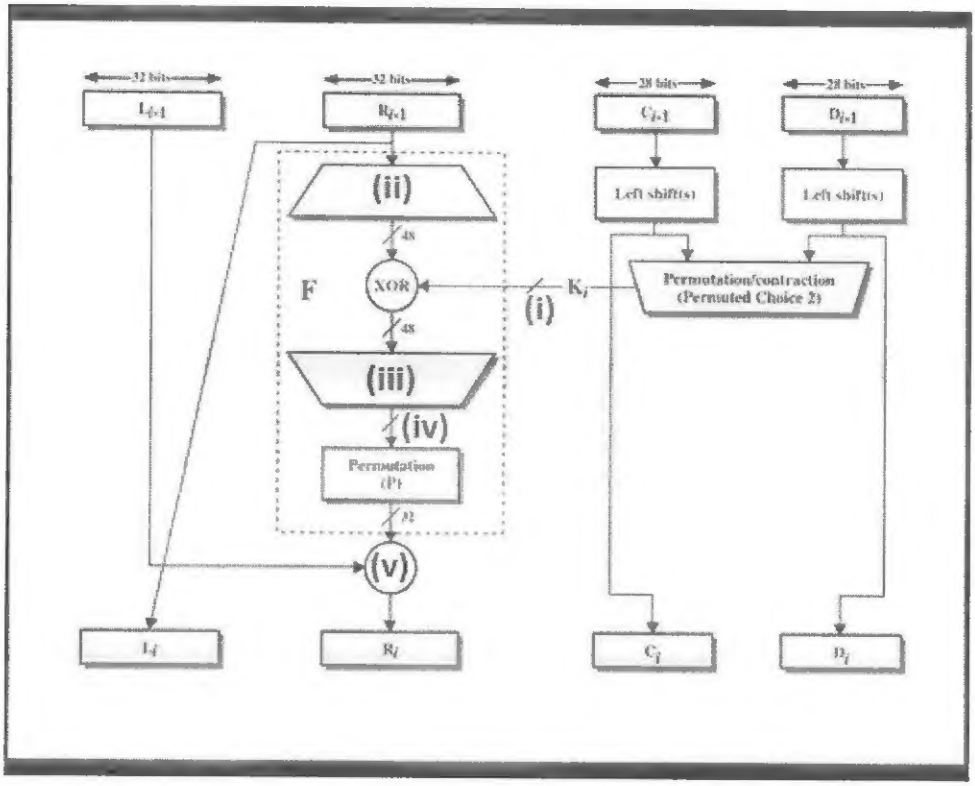
monkey see monkey do

[3 marks]

Continued ...

d) The Data Encryption Standard (DES) Round Function is shown diagrammatically below.

[10 marks]



Answer the following:

(i) How many bits are represented (for K_i)?
(ii) What is the name (or function) of (ii)?
(iii) What is the name (or function) of (iii)?
(iv) How many bits are represented at (iv)?
(v) What is the operation at (v)?

Continued ...

Question 3 (20 Marks)

a) Miller Rabin Algorithm is a test based on the Fermat's Theorem. The Miller-Rabin Algorithm is as described below.

The test for (n) is:

1. Find integers k, q such that $k > 0$, q is an odd number, so that $(n-1)=2^k q$
2. Select a random integer a, where $1 < a < n-1$
3. if $a^q \bmod n = 1$ then return ("maybe prime");
4. for $j = 0$ to $k - 1$ do
    5. if $(a^{2^j q} \bmod n = n-1)$
        then return("maybe prime")
6. return ("composite")

Using the algorithm above, show how you will test for the number 15 by choosing a random integer *a*. Show how you obtain your result clearly.

[10 marks]

b) Why are probabilistic considerations required when using the Miller-Rabin Algorithm?

[2 marks]

c) Explain, in your own words, why one-way hash functions (e.g. MD-5 or SHA-512) are used for password storage. To enhance the password storage, what is the function of the cryptographic salt?

[4 marks]

d) To protect against inference attacks, database systems can control individual data access. This is basically a trade-off between security and precision. There are TWO (2) main methods that can be applied to the data. List the TWO (2) methods and provide an explanation for each one.

[4 marks]

Continued ...

Question 4 (20 Marks)

a) Risk analysis is process of identifying the loss (lost productivity, loss of quality, financial loss, etc.) if a security breach occurs, accessing the likelihood of an event happening and formulating controls to reduce the impact. However, there are reasons on why an organization should not conduct risk analysis. State at least 2 reasons why risk analysis should not be conducted.

[2 marks]

b) Briefly describe 6 (out of the 7) issues that are addressed by a security plan.

[6 marks]

c) In the protection of intellectual property; describe Patent, Copyrights and Trademarks.

[6 marks]

d) Provide the appropriate Intellectual Property protection that can be applied to the following scenario.

- Justin has thought of a new algorithm to determine the risk of a (car) driver which will be useful for insurance companies. He has coded the algorithm but is unable to test it as he does not have access to actual insurance data on drivers' profile and claims history. However, he would like to sell it to insurance companies but he also needs the data from the insurance companies. The insurance company needs assurance that his algorithm works and has asked him to present his solution to them, including how his algorithm works. Justin wants to protect his algorithm and setup a company to market the software but is unsure how. He has come to you to ask for advice.

What would you advise him to do?

[4 marks]

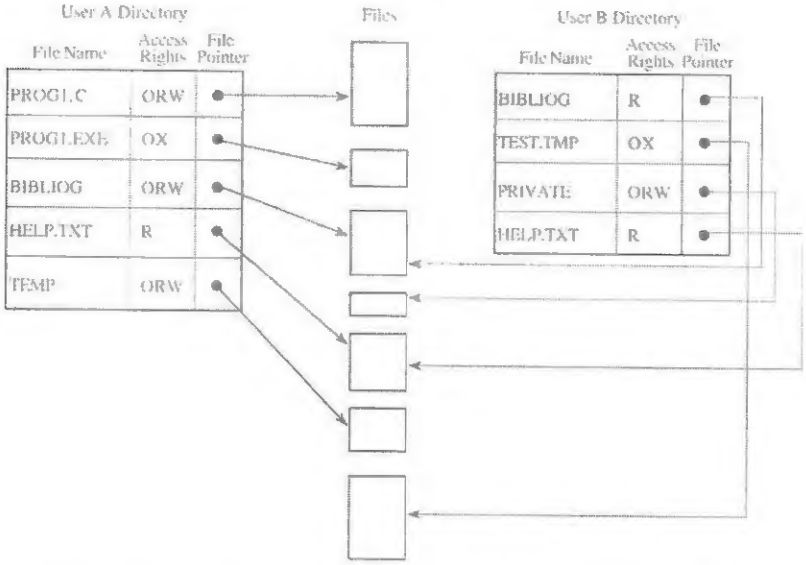
e) Explain what One-Time Password is and how it addresses at least ONE (1) of the shortcomings of using traditional (static) passwords.

[2 marks]

Continued ...

Question 5 (20 Marks)

a) One of the simplest methods for file protection is to implement a directory listing of file permissions. This is a global list kept by the operating system and it is easy to implement, using one list per user in the system. This is illustrated below:-



What are the THREE (3) drawbacks for such an implementation?

[3 marks]

b) Briefly explain what is meant by "loose-lip" in assisting a password attack?

[2 marks]

c) What is meant by a two-factor authentication and give an example of it by explaining which of the two-factors are used.

[3 marks]

d) Network Based IDS are generally implemented in stealth mode. Give a detailed explanation what this means and how does it work (use a diagram to illustrate).

[4 marks]

e) Pretty Good Privacy (PGP) was designed to provide *confidentiality*, *authenticity* and *integrity* of plaintext email messages. Describe in detail the process of using PGP and indicate how the *confidentiality*, *authenticity* and *integrity* are achieved in the process.

[8 marks]

END OF EXAM PAPER